⑲日本国特許庁(JP)　⑪特許出願公開

⑫公開特許公報(A)　平4−72840

⑤Int.Cl.[5]　識別記号　庁内整理番号　⑬公開　平成4年(1992)3月6日

H 04 L 9/06
9/14

7117−5K　H 04 L 9/02　Z

審査請求　未請求　請求項の数 1　(全5頁)

⑭発明の名称　データ伝送方法

⑳特　願　平2−185076

㉒出　願　平2(1990)7月12日

⑫発明者　松田　義巳　京都府京都市右京区梅津高畝町47番地　日新電機株式会社内

⑪出願人　日新電機株式会社　京都府京都市右京区梅津高畝町47番地

⑭代理人　弁理士　藤田　龍太郎

明　細　書

1　発明の名称

データ伝送方法

2　特許請求の範囲

① 送信側により数字，文字等の送信データを暗号鍵を用いて順次に暗号化して送信し、受信側により暗号化された受信データを復号鍵を用いて順次に復号化するデータ伝送方法において、

送信側に複数の暗号鍵を保持した暗号鍵管理部を設けるとともに、受信側に前記暗号鍵管理部の各暗号鍵に対応する複数の復号鍵を保持した復号鍵管理部を設け、

暗号化する送信データの計数に基づき、前記暗号鍵管理部の各暗号鍵を一定数の送信データの暗号化毎に順次に選択して暗号化の鍵を周期的に順次に変更し、

復号化した受信データの計数に基づき、前記復号鍵管理部の各復号鍵を一定数の受信データの復号毎に順次に選択し、復号化の鍵を前記暗号化の鍵の変更に連動して順次に変更する

(1)

ことを特徴とするデータ伝送方法。

3　発明の詳細な説明

〔産業上の利用分野〕

本発明は、数字，文字等のデータを送信側の暗号鍵，受信側の復号鍵を用いた暗号化方式で暗号化して伝送するデータ伝送方法に関する。

〔従来の技術〕

従来、この種鍵を用いた暗号化方式のデータ伝送は、第2図に示すように送信側の暗号化装置(1A)と受信側の復号化装置(2A)とを無線又は有線の伝送路(3)で結合して行われる。

そして、暗号化装置(1A)は暗号化部(4)及びメモリ等で形成された暗号鍵管理部(5A)を備え、この管理部(5A)は上位装置又は人手の書込みによって与えられた特定データの1個の暗号鍵を保持する。

また、復号化装置(2A)は復号化部(6)及びメモリ等で形成された復号鍵管理部(7A)を備え、この管理部(7A)は暗号鍵に対応する1個の復号鍵を保持する。

そして、暗号化装置(1A)の数字，文字等の送信

(2)

データDiは順次に暗号化部(4)に送られ、この暗号化部(4)により暗号鍵管理部(5A)の暗号鍵を用いて暗号化される。

この暗号化は、例えば送信データDiと暗号鍵のデータKaとの四則演算により施される。

そして、暗号化された送信データDiは、伝送路(3)を介して復号化装置(2A)に順次に伝送される。

つぎに、復号化装置(2A)においては、暗号化された送信データDiが受信データとして順次に復号化部(6)に供給される。

そして、復号化部(6)により、復号鍵管理部(7A)の復号鍵を用いて受信データが復号化され、送信データDiと同一の復号データDoが再生される。

なお、復号化は、例えば復号鍵のデータKbを用いた暗号化の逆演算により施される。

〔発明が解決しようとする課題〕

前記従来のデータ伝送方法の場合、暗号鍵，復号鍵が1組だけ用いられるとともに、両鍵の内容（データ）は上位装置又は人手で書換えられない限り変わらない。

そして、暗号化と復号化との鍵の不一致に基づく復号化ミス等を防止するため、少なくともデータ伝送中に両鍵の内容が書換えられて変更されることはなく、通常は両鍵が初めに与えられた内容に固定されて用いられる。

したがって、例えば管理部(5A)，(7A) の書込み時に両鍵それぞれのデータKa，Kb が盗まれたりすると、極めて簡単に暗号解読が行われてデータが盗用され、機密保持の信頼性が低い問題点がある。

本発明は、暗号鍵，復号鍵を周期的に変更し、機密保持の信頼性を向上するようにしたデータ伝送方法を提供することを目的とする。

〔課題を解決するための手段〕

前記目的を達成するために、本発明のデータ伝送方法においては、送信側に複数の暗号鍵を保持した暗号鍵管理部を設けるとともに、受信側に前記暗号鍵管理部の各暗号鍵に対応する複数の復号鍵を保持した復号鍵管理部を設け、

暗号化する送信データの計数に基づき、前記暗号鍵管理部の各暗号鍵を一定数の送信データの暗

号化毎に順次に選択して暗号化の鍵を周期的に順次に変更し、

復号化した受信データの計数に基づき、前記復号鍵管理部の各復号鍵を一定数の受信データの復号毎に順次に選択し、復号化の鍵を前記暗号化の鍵の変更に連動して順次に変更する。

〔作　用〕

前記のように構成された本発明のデータ伝送方法の場合、暗号鍵管理部，復号鍵管理部には、従来と異なり、複数の暗号鍵，復号鍵それぞれが保持される。

そして、各暗号鍵及び各復号鍵をそれぞれ1番目，2番目，3番目，…，N番目の鍵とすると、最初は1番目の暗号鍵，復号鍵が選択されて両鍵を用いた暗号化，復号化が行われる。

また、暗号化する送信データ，復号化した受信データの計数に基づき、暗号化，復号化のデータ数が計数される。

そして、一定数の送信データの暗号化が終了すると、2番目の暗号鍵が選択されて送信側の暗号

化の鍵が自動的に変更される。

また、一定数の暗号化された送信データに基づく一定数の受信データの復号化が終了すると、2番目の復号鍵が選択されて受信側の復号化の鍵も自動的に変更される。

以降、一定数の送信データが暗号化される毎に、暗号化の鍵が3番目，…，N番目，1番目，2番目，…の暗号鍵に順次に変更されるとともに、この変更に連動して復号化の鍵も3番目，…，N番目，1番目，2番目，…の復号鍵に変更される。

そして、暗号化，復号化の鍵がそれぞれ複数になり、しかも、データ伝送中に両鍵が変更の順序と周期との組合わせで周期的に順次に変わるため、例えば暗号鍵管理部，復号鍵管理部の書込み時に鍵のデータが盗まれても、容易には暗号解読が行えず、機密保持の信頼性が向上する。

〔実施例〕

1実施例について、第1図を参照して説明する。

第1図において、(1B)，(2B) は第2図の装置(1A)，(1B) に相当する暗号化装置，復号化装置で

あり、暗号化部(4)，復号化部(6)それぞれを有する。

(8)は暗号化部(4)の前段に設けられた送信データ計数用のカウンタ、(5B)は第2図の管理部(5A)の代わりに設けられた暗号鍵管理部であり、順次のアドレスA_1，A_2，…，Anに1番目，2番目，…，N番目の暗号鍵のデータKa_1，Ka_2，…，Kanを保持する。

(9)は復号化部(6)の後段に設けられた受信データ計数用のカウンタ、(7B)は第2図の管理部(7A)の代わりに設けられた復号鍵管理部であり、順次のアドレスA_1，A_2，…，An に管理部(5B)の各暗号鍵それぞれに対応する各復号鍵のデータKb_1，Kb_2，…，Kbn を保持する。

そして、管理部(5B)，(7B) はそれぞれメモリ等で形成され、上位装置又は人手により予め各暗号鍵のデータKa₁～Kan，各復号鍵のデータKb₁～Kbnが書込まれる。

また、カウンタ(8)，(9)はそれぞれリングカウンタ等で形成され、暗号化前の送信データ，復号化後の受信データそれぞれを設定された一定数M(=1，2，…の整数) 計数する毎にアドレスA_1，A_2，…，An

に順次に変化する鍵選択信号Ax，Ayを管理部(5B)，(7B)に出力する。

そして、データ伝送が開始されると、装置(1B)，(2B)のスタート操作等によってカウンタ(8)，(9)が0又はMに初期化され、鍵選択信号Ax，Ay が共にアドレスA_1の信号になる。

このとき、管理部(5B)から暗号化部(4)に1番目の暗号鍵のデータKa_1 が読出されるとともに、管理部(7B)から復号化部(6)に1番目の復号鍵のデータKb_1 が読出され、暗号化の鍵及び復号化の鍵の初期設定が行われる。

そして、カウンタ(8)を介して暗号化部(4)に送信データDiが供給されると、送信データDiの通過毎にカウンタ(8)がアップカウント又はダウンカウントするとともに、送信データDiが1番目の暗号鍵を用いて暗号化される。

さらに、暗号化された送信データDiは、伝送路(3)を介して復号化装置(2B)に順次に伝送される。

そして、受信した送信データDiは受信データとして復号化部(6)に供給され、この復号化部(6)によ

り、受信データが1番目の復号鍵を用いて正しく復号化される。

また、受信データの復号化によって形成された復号データDoがカウンタ(9)を介して再生出力され、このとき、復号データDoの通過毎にカウンタ(9)がカウントアップ又はカウントダウンする。

そして、M個の送信データDiが1番目の暗号鍵を用いて暗号化され、一定数の暗号化が終了すると、カウンタ(8)は鍵選択信号AxがアドレスA_2の信号に変化して計数内容が0又はMに戻る。

さらに、鍵選択信号Axの変化に基づき、管理部(5B)から読出される暗号化の鍵Kaxは、M番目の送信データDiの暗号化直後に2番目の暗号鍵のデータKa_2に変わる。

また、前記M番目の送信データDiに基づく受信データが1番目の復号鍵を用いて復号化され、一定数の復号化が終了すると、この復号化によって形成されたM番目の復号データDoの通過に基づき、カウンタ(9)は鍵選択信号AyがアドレスA_2の信号に変化して計数内容が0又はMに戻る。

そして、鍵選択信号Ayの変化に基づき、管理部(7B)から読出される復号鍵のデータKby も2番目の復号鍵のデータKb_2に変わる。

したがって、つぎのM個の送信データDiは2番目の暗号鍵を用いて暗号化され、この暗号化に基づくM個の受信データは2番目の復号鍵を用いて復号化される。

以降、M個の送信データDiの暗号化が終了する毎に、カウンタ(8)の鍵選択信号Axがつぎのアドレスの信号に変わり、暗号化の鍵が3番目，…，N番目，1番目，2番目，…の暗号鍵に自動的に順次に変更される。

また、復号化された受信データ，すなわち復号データDoの計数に基づき、M個の受信データの復号化が終了する毎に、カウンタ(9)の鍵選択信号Ayがつぎのアドレスの信号に変わり、復号化の鍵も暗号化の鍵の変更に連動して3番目，…，N番目，1番目，2番目，…，の復号鍵に自動的に順次に変更される。

そして、データ伝送中に暗号化の鍵が設定され

た順序で周期的に変わるため、暗号鍵のデータKa₁～Kan，復号鍵のデータKb₁～Kbnが盗まれても、それらの変更の順序及び周期が分らず、暗号解読は容易でない。

なお、解読を一層困難にするため、変更の周期については、送信データDiのビットパターンの出現状況等を考慮して調整することが望ましい。

〔発明の効果〕

本発明は以上説明したように構成されているため、以下に記載する効果を奏する。

暗号鍵管理部(5B)，復号鍵管理部(7B)に複数の暗号鍵，復号鍵を保持し、送信データの一定数の暗号化毎に管理部(5B)の各暗号鍵を順次に選択して暗号化の鍵を周期的に順次に変更するとともに、受信データの一定数の復号化毎に管理部(7B)の各復号鍵を順次に選択し、復号化の鍵を暗号化の鍵の変更に連動して順次に変更したため、伝送中に暗号化の鍵を自動的に変更して暗号化方式のデータ伝送が行え、このとき、暗号解読が容易に行えず、機密保持の信頼性が著しく向上する。

(11)

4 図面の簡単な説明

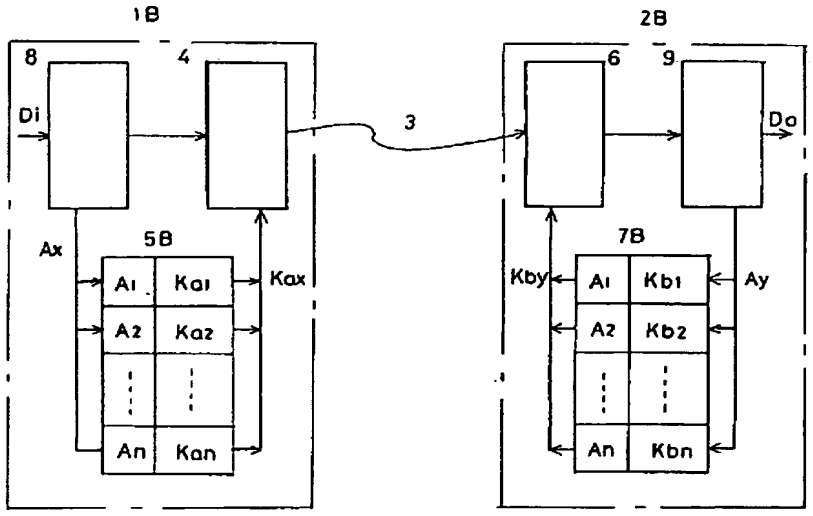
第1図は本発明のデータ伝送方法の1実施例のブロック図、第2図は従来例のブロック図である。

(1B)…暗号化装置、(2B)…復号化装置、(3)…伝送路、(4)…暗号化部、(5B)…暗号鍵管理部、(6)…復号化部、(7B)…復号鍵管理部、(8)，(9)…カウンタ。

代理人　弁理士　藤田　龍太郎

(12)

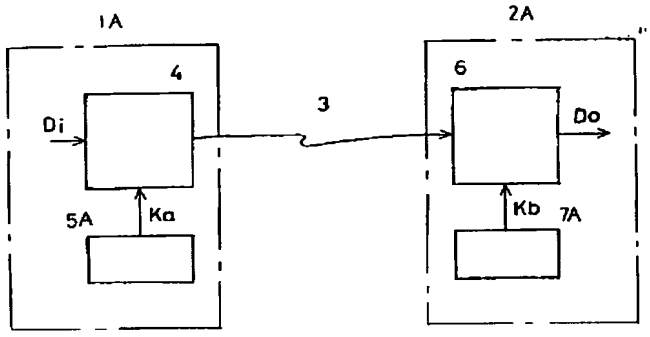
第 1 図



1B --- 暗号化装置
2B ---復号化装置
3 --- 伝送路
4 --- 暗号化部
5B --- 暗号鍵管理部
6 --- 復号化部
7B ---復号鍵管理部
8,9 ---カウンタ

49200231 引用例・公知例

第 2 図



1A --- 暗号化装置
2A --- 復号化装置
5A --- 暗号鍵管理部
7A --- 復号鍵管理部